Sumomo: ブロックチェーンを用いた教育用オンラインジャッジの提案

松本　彩花[1,a)]　松原　南美[2]　渡邉 遥輔[3]　多田　拓[3]　倉光　君郎[1,b)]

概要：
近年, オンラインジャッジはプログラミング学習者に良い自習ツールとして, 世界中で使用されている. プログラミング教育者の観点からも, 大きな利点が期待される. しかし, 課題として,「問題セットの自由度が低い」,「学習歴を活用しにくい」ことが挙げられる. ゆえに, 本研究では, ブロックチェーン を用いたオンラインジャッジを提案する. ブロックチェーン適用の利点は「データ改竄防止」,「特定の機関に依存しない」,「学習歴が保護される」等である. これにより, 教育組織に依存なしに問題セットを追加し, 学習歴を参照しやすいオンラインジャッジを実現する.

Sumomo: A online judge for education with block chain

Ayaka Matsumoto[1,a)]　Minami Matsubara[2]　Yousuke Watanabe[3]　Taku Tada[3]
Kimio Kuramutsu[1,b)]

Abstract:
Recently, many online judges have been provided as self-studying tool for programming learners. There are several benefits for teachers to use online judge. However, there are some problems to use online judge system such as "low-flexibility of problem sets" and "low-utilizable of study log". Our study will propose a new online judge integrated emerging of block chain, which can realize more value-added reputation toward students. Application block chain has many benefits such as "data tamper resistance", "no-dependence toward particular authority", "highly protect-ability of study logs". Hence, we will introduce a new online judge which easy to refer study log, and add problem sets without dependence of educator.

1. はじめに

（背景）オンラインジャッジは, プログラムの正誤を入出力から判定するシステムである. 競技プログラミング大会やその練習会で利用されている. このオンラインジャッジは, プログラミング学習者にとってよい自習ツールとなる. 加えて, プログラミング教育者にとっても, 学習者の個々の進捗を把握し, 多くの学生がつまずいている箇所をリアルタイムで把握できるなど, 指導のためのツールとなる.

現在, オンラインジャッジは,AOJ ? や AtCoder などの大学や民間企業から提供されている. しかし, そもそもの目的が競技向けであり教育向けではない部分も多い. 例えば,Python 入門向けの講座で利用したとき次のような難点がある.

- 競技会の過去問が集まっているため問題セットの難易度が高すぎる
- C/C++ 用の問題が多く Python では書きにくいことが多い. 言い換えると,Python を用いると計算処理の

[1] 日本女子大学大学院
Mathematical and Physical Properties Science, Graduate School of Science, Japan Women's University Graduate School, 2-8-1 Mejirodai, Bunkyo-ku, Tokyo 112-868, Japan
[2] 日本女子大学
Department of Mathematical and Physical Sciences, Japan Women's University, 2-8-1 Mejirodai, Bunkyo-ku, Tokyo 112-868, Japan
[3] 横浜国立大学大学院理工学府
Graduate School of Engineering, Yokohama National University, 79-1 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa 240-8501, Japan
a) m1416086ma@ug.jwu.ac.jp
b) kuramitsuk@fc.jwu.ac.jp

速度が遅く, ランタイムエラーになってしまうことがある. ローカル環境にて実行可能であっても, プログラムの実行速度によって, オンラインジャッジ上では実行不能になる場合がある.

- プログラム実行環境がサーバに固定されライブラリなどを追加できない.

オンラインジャッジは, 教育システムとして可能性があるが, 現状では使いにくいものである.

（目的）本研究の目的は, より自由度の高い教育向けオンラインジャッジの提案である. ここで「自由度の高い」とは, ライブラリの制約がなく, 教育組織に依存せず問題セットを追加し, 学習歴を共有できることを意味する.

（方法）我々は, 高い自由度を実現するため, 自律分散型のオンラインジャッジとブロックチェーンによる学習歴と個人情報の保護の共有を行うことを提案する.

ブロックチェーンとは, 分散型台帳とも呼ばれ, 複数人の管理者によってデータベースの一部である台帳情報を共有して管理する技術のことである. 仮想通貨が有名であるが, スマートコントラクトと呼ばれるプログラムを書くことで, 仮想通貨以外のアプリケーションに応用が可能である.

本稿では, ブロックチェーンと統合した自律分散型のオンラインジャッジ Sumomo の試作を報告する. Sumomo では, ローカル環境でプログラムを実行＆判定し, その結果をブロックチェーンに学習歴として記録する. 問題セットは,Github 上で公開すれば誰でも公開可能になる. ローカル環境で実行するため, 不正プログラムによるセキュリティリスクを気にすることなく, 多様なライブラリを含めた問題の作成が可能になる. 一方, 学習歴はブロックチェーン上で記録されるため, ブロックチェーンの機能により匿名化し保護される. ユーザが許可すれば, 学習歴は成績評価からプログラミング能力の保証まで, 様々な付加価値サービスに活用が可能になる. 本稿の残りは以下の通りである.

本稿では, ブロックチェーンと統合した自律分散型のオンラインジャッジ Sumomo の試作を報告する. 第 2 節では, オンラインジャッジの教育向け利活用について述べる. 第 3 節では, ブロックチェーン技術を概観する. 第 4 節では,Sumomo の設計と実装状況を報告する. 第 5 節は, 本稿をまとめる.

2. オンラインジャッジ

オンラインジャッジ？？？は, 競技プログラミングにおいて同一環境で公平にプログラムの正誤判定と性能審査をするシステムである. 主目的はプログラミング競技会での審査のためであるが, 教育用途を含め様々なバリエーションが開発されている. 本稿は, 著者らが大学教育で利用してきた経験をもとに, 会津オンラインジャッジ (以下,AOJ) を参照例に説明する.

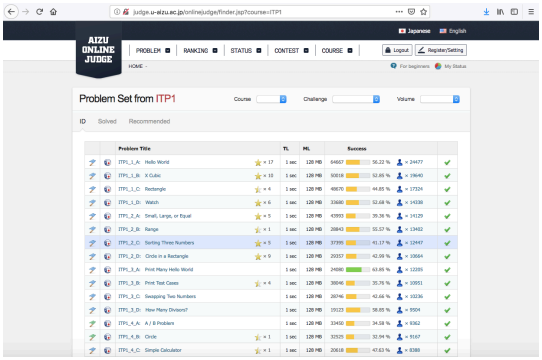

図 1　AOJ の画面例

2.1 AOJ

AOJ ?は, 会津大学において提供されるオンラインジャッジである. 過去の各種プログラミング競技会の過去問 (ICPC, PCK, JOI) をアーカイブするだけでなく, ITP(Introduction To Programming) と呼ばれる入門者向けの問題集も提供している. 多くの学生がプログラミングの練習に利用しているため, 国内の主要なオンラインジャッジのひとつとなっている. 図 1 では,AOJ の問題の例である.

利用者は, 問題文を読んで手元のプログラミング環境で解答プログラムの作成を行う. （AOJ は, 開発環境は付属していない.）手元でプログラムができたら,AOJ に提出する. すると, サーバ側でテストデータの照合を行い, 基本的に合否のみ通知される. 否定の場合は, システムが補足するエラーの種類を Wrong Answer, Runtime Error, Time Limited Exceed として返すが, エラーメッセージを含めた詳細はわからないようになっている. 利用者のジャッジ結果は, 全てデータベースとしてサーバに蓄積される. このデータベースは, 公開されており,Web API を経由して取り出すことができるようになっている.

2.2 教育への応用例

著者らは,2018 年度より, 日本女子大学理学部数物科学科の 4 クラスにおいて, AOJ を用いたプログラミング演習を導入している.

- 言語 C/C++ もしくは Python (クラスにより異なる)
- ITP (Introduction To Programming) 約 40 問を解答する
- 進んだ学生向けに、PCK, JOI, ICPC から簡単な問題を選んで解答する

我々は,AOJ の提供する Web API を用いて, ユーザ名から, 問題番号, 解答時刻, 解答言語, 解答結果などの情報を得ている.

表 1 は,2019 年度クラス (4 週目) の解答数と演習時間の抜粋である. 表 2 は, 同年同時期の問題ごとの不正解数/正解数と不正解を出しているユーザ名のリストである. このように学生の在宅学習を含めた進捗を把握することがで

表 1　解答数と演習時間 (例)

ユーザ名	C++	Python	時間
guog**	38	0	49
haku***	3	41	38
hono***	26	0	36
hiyo**	0	47	30
aben*	0	34	28
tefu***	4	33	25
ai03**	23	0	24
soku*****	0	19	21
yusm**	29	0	20
umin***	3	20	17

表 2　問題ごとの正解数と助けが必要な学生

問題番号	不正解者 / 正解者数	不正解者
ITP1_1_A	4 / 48	nagi****,etc...
ITP1_1_B	1 / 57	ayan**’
ITP1_1_C	1 / 50	yasu****
ITP1_2_A	4 / 45	mapl***,etc...
ITP1_2_B	1 / 45	cbji* ,etc...
ITP1_2_C	9 / 35	meru**,etc...
ITP1_2_D	4 / 23	rn10**, meru**,etc...
ITP1_3_A	1 / 43	rila*****
ITP1_3_B	2 / 17	kimu****, rt56**
ITP1_3_C	2 / 41	yuko****, ayar**
ITP1_4_A	1 / 45	yuko****
ITP1_4_B	2 / 13	ayar**, rt56**
ITP1_4_C	2 / 9	yuko****, mio3*
ITP1_4_D	4 / 4	yuko****,etc...

きる.

AOJ は, 教育システムとして高いポテンシャルを持っている. 特に,AOJ に蓄積される学習歴は, 教育機関を超えてプログラミング能力を測る指標となる. これらがモチベーション (インセンティブ) となって, 学習が進むことが見受けられる.

AOJ は, もともと教育向けに設計されたシステムでないため, 限界もある. AOJ は, 多くの問題文をアーカイブしているが, 分野の偏りがある. 必要に応じ, 外部から問題を追加することもできない. また, 競技者の公平性を保つため, ライブラリの利用を制限し, 標準環境よりも不自由なプログラム実行環境になっている. この点も, プログラム課題の自由度の制約となっている.

3. ブロックチェーン

本節では, ブロックチェーン?について簡単に紹介する.

3.1 概要

ブロックチェーンは, 複数の管理者によるコンセンサスアルゴリズム (合意形成) によって, 分散型のデータ管理を実現している技術である. 主な特徴としては「データの改竄防止」に強みがある点,「1 つの組織に依存なし」にデータ管理ができる点,「ユーザの匿名性を担保できる」点などが挙げられる.

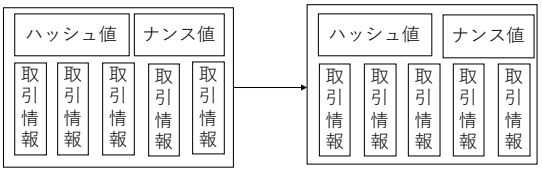

図 2　ブロックチェーンのデータ構造

ブロックチェーンは, ハッシュ値によって連鎖されたデータ構造 (図 2) である. 取引情報は, そもそも仮想通貨による出入金を記録するものであったが, ここに学習歴などのデータも記録できるように一般化されている. ハッシュ値の連鎖は, ある条件を満たすハッシュ値が必要であり, ナンスと呼ばれる乱数生成をしながら計算する. この計算量が大きく設定されているため, ハッシュ値の連鎖は非決定的かつ分散的に行われる.

ブロックチェーンは, 原理的に非中央的であり, 記録の改竄を防ぐことができる. 一つの組織に依存することなくデータを共有することができ, 仮想通貨とあわせてデータの取引も実現しやすい. 一方, 適切なアカウントとデジタル証明を用いることで, 十分な本人確認性と匿名性を実現することもできる.

3.2 ブロックチェーンの応用例

ブロックチェーンは, もともと仮想通貨 (ビットコイン) の実装基盤として開発された. しかし, 直ぐに通貨以外のデータを保持する用途に応用が広がった.

代表的なブロックチェーンの応用には次のようなものがある.

- 金融・保険産業
- IoT 家電
- 農業ログ

また, 上記の利点から教育分野への応用?が始まっている. 学校情報ハブの設計?にブロックチェーンが用いられている. ブロックチェーンで学習歴の収集や記録をすることによって, 正確な意思決定や詐称行為を防ぐことを目的としている.

4. Sumomo

4.1 概要

Sumomo は, 我々が開発を進める学校教育用オンラインジャッジの試作システムである. プログラミング環境とジャッジが統合されたプログラミング学習のためのプラットフォームである. 主な目的は, 初学者がプログラミング学習に取り組みやすく, 教師が授業で使いやすいことである. さらに, 学生の就職活動にも役立つことを目指している.

表 3　Sumomo と AOJ の比較表

	Sumomo	AOJ
問題セットの自由度	○	×
プログラミング環境	○	×
実行環境（ライブラリ追加）の自由度	○	×
実行エラーの詳細	○	×
ユーザの匿名性	○	○
学習歴の保存と共有	○	○
不正行為	×	×

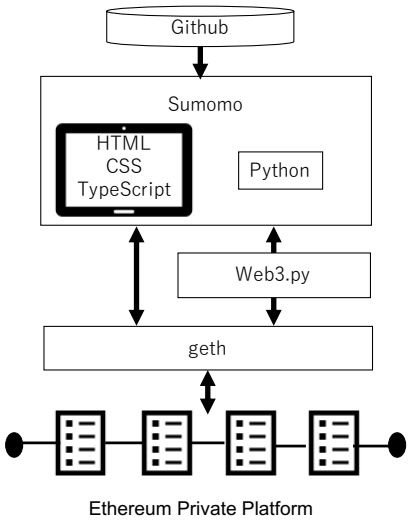

図 3　Sumomo のシステム概要

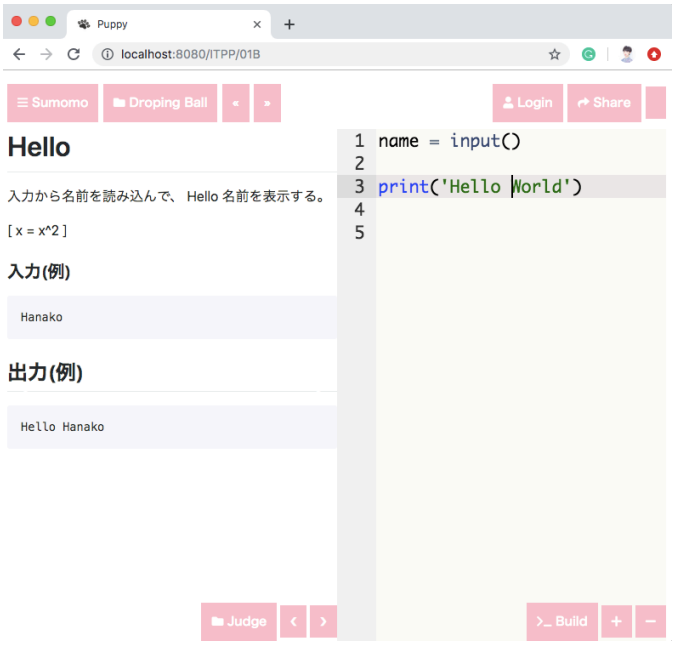

図 4　Sumomo の画面例

Sumomo が想定とするユーザは学生, 教師, 企業の人事部である. 学生は学習歴追加し, 更新した学習歴を参照する.

教師は, 学生が更新した学習歴を把握し, 成績評価に反映する. 人事部は, 学習歴参照し, 採用に反映できる.

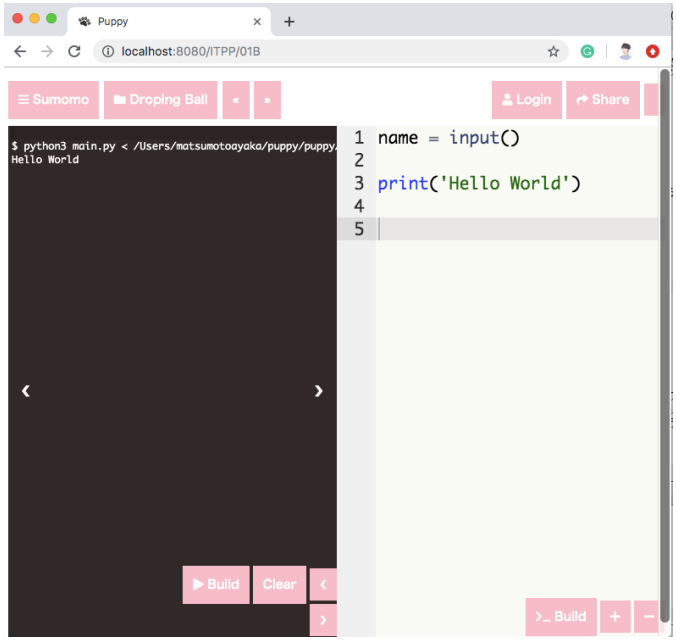

図 5　Sumomo の画面例

4.2　問題セットの配布

問題セットは, オープンソースの標準的な配布手段である Github を用いて配信する. 教師は, 所定の様式に従い問題とジャッジデータ (入出力) を用意する. 問題の記述は, 標準的な Markdown を用いる.

4.3　統合プログラミング環境

Sumomo はブロックチェーンと統合したローカルなプログラミング環境を提供する. 以下にローカル環境とブロックチェーンのそれぞれの機能範囲を示す.

- **ローカル環境**
  学生がローカル環境でプログラミングからジャッジまでを行う. ローカル環境で実行する為, 実行性能・使用リソースの制限はかけない. Sumomo 画面から利用者は Web ブラウザを通して, 図 4 の画面左側の問題を読み, 右側のエディタでコードの編集を行う. ソースコード実行は, 図 5 の画面左側のコマンドプロンプトで行う. 現在は, システムの試作として Flask によるローカル Web サーバを立ち上げて,Web ブラウザとのインタラクション, ジャッジプログラムの実行を行なっている.
- **ブロックチェーン**
  学生が学習歴追加・学習歴参照を行い, 教師が学習歴参照し成績評価に反映できる. 人事部は学習歴参照を行い, 採用活動に利活用することができる. また, 学習歴にはアクセス制限をかけ, 人事部が学生の学習歴を参照する際に学習歴アクセス許可を学生に要請する必要がある.

4.4 Ethereum

Sumomo は, 本稿の執筆時点で,Ethereum を採用し, ブロックチェーンの学習歴を記録することを計画している. Ethereum は, オープンソースの分散型アプリケーション基盤実行可能なブロックチェーン基盤である. Ethereum との接続は, 図 3 のようになっている. ローカル環境と Ethereum プラットフォームは Python 言語の web3 モジュールで接続されている.

チューリング完全な計算能力を持つ Solidity 言語でスマートコントラクトと呼ばれるプログラムを書くことで, 様々な分野のブロックチェーン応用が実現可能になっている.

本研究では, 学習歴と個人情報を保持するコントラクトを作成する. コントラクトには以下を記録する.

- ユーザ ID
- 問題 ID
- ジャッジ結果
- ジャッジした結果のハッシュ値
- ジャッジしたコードのハッシュ値

Sumomo システムは, パーミッション型で運用することを想定している. パーミッション型にすることによって, 特定の参加者のみでネットワークを作り, 学習歴参照できるのは参加者のみに限定できる. ただし, 現在はプライベート型のブロックチェーンで検証を行なっている.

5. むすびに（検討課題)

Sumomo の構想と試作システムについて述べた. Sumomo は, 教育分野で利用しやすいように, 意識して開発が進められている.

ブロックチェーンとの連携は, ジャッジ結果の安全な共有に用いているのみである. 仮想通貨などのインセンティブとの連携はまだ検討が始まったばかりである. 今後は, 問題セットの開発とシステム評価を進める.

システムの評価には, アンケートによる標本調査または学校の授業にて使用する実証実験による評価を考えている.

謝辞 若杉祐依さん (日本女子大学大学院理学研究科数理・物性構造科学専攻)、秋信有花さん、坂根万琴さん（日本女子大学理学部数物科学科）から AOJ の利用体験に関する助言を頂きました.